Mathematics for Computer Science

MIT 6.042J/18.062J

Truth & Proof

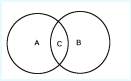
Math vs. Reality

Propositional Logic

Team Problem

Surprise Problem 1

Math



Sets

Numbers $4, \sqrt{7}, \pi, i+1$

T*, *F Booleans

Strings `"albert meyer"`

$f(x) ::= x^2 + 2$ Functions

Relations $a \le b$

Data structures

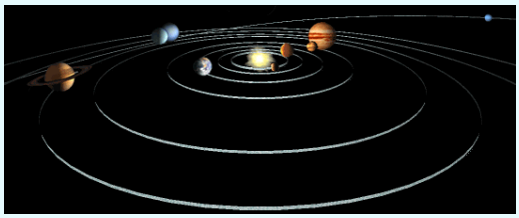
Not Math

Family

Not Math

Cats

Not Math



Solar System

Not Math: *Cogito ergo sum*

René Descartes'
MEDITATIONS
on First Philosophy in which the Existence of God and the Distinction Between Mind and Body are Demonstrated.

(Picture source: http://www.btinternet.com/~glynhughes/squashed/descartes.htm)

 February 9, 2007 lec 1F.7

Evidence vs. Proof

Let $p(n) ::= n^2 + n + 41$.

Claim:

$\underbrace{\forall\, n}\ \underbrace{\in \mathbb{N}}.\ p(n)$ is a prime number

for all n that are *nonnegative integers*

 February 9, 2007 lec 1F.8

Only Prime Numbers?

Evidence:

$p(0) = 41$	prime	
$p(1) = 43$	prime	
$p(2) = 47$	prime	
$p(3) = 53$	prime	
⋮		
$p(20) = 461$	prime	**looking good!**
⋮		
$p(39) = 1601$	prime	**enough already!**

 February 9, 2007 lec 1F.9

Only Prime Numbers?

$\forall\, n \in \mathbb{N}.\ p(n) ::= n^2 + n + 41$
is a prime number

This is not a coincidence.
The hypothesis must be true. *But no!*

$p(40) = 1681$ is *not prime*.

 February 9, 2007 lec 1F.10

Only Prime Numbers?

Quickie:
Prove that 1681 is not prime.

Proof: $1681 = p(40)$
$= 40^2 + 40 + 41$
$= 40^2 + 2 \cdot 40 + 1$
$= (40 + 1)^2$

 February 9, 2007 lec 1F.11

Further Extreme Example

Hypothesis:
$313 \cdot (x^3 + y^3) = z^3$
has no solution in positive integers

False. But smallest counterexample
has more than 1000 digits!

 February 9, 2007 lec 1F.14

P = NP?

- Overwhelming evidence for $\neq$ based on centuries of experience
- Modern cryptography (like RSA) depends on $\neq$
- Nearly all experts believe $\neq$
- But *mathematically* unproven – the most important open problem in CS

Propositional (Boolean) Logic

Proposition is either **True** or **False**

Examples: $2+2=4$ True

$1\times 1=4$ False

Non-examples: Wake up!

Where am I?

Operators

$\wedge$ ::= AND

$\vee$ ::= OR

$\neg$ ::= NOT

$\rightarrow$ ::= IMPLIES (if …then)

$\leftrightarrow$ ::= IFF (if and only if)

English to Math

"If Greeks are Human, and Humans are Mortal, then Greeks are Mortal."

$$((G \rightarrow H) \wedge (H \rightarrow M)) \rightarrow (G \rightarrow M)$$

English to Math

Greeks carry Swords or Javelins

$$(G \rightarrow S) \underbrace{\vee} (G \rightarrow J)$$

disjunction

True even if a Greek carries both

English to Math

Greeks carry Bronze or Flint swords

$$(G \rightarrow B) \underbrace{\oplus} (G \rightarrow F)$$

exclusive-or

$P \oplus Q$ means "P or Q but not both"

Math vs. English

Parent: If you don't clean your room (C), you can't watch a DVD (D)."

$$\neg C \longrightarrow \neg D$$

$$C \longrightarrow D \;?\; \text{YES!}$$

Math vs. English

Parent: If you don't clean your room (C), you can't watch a DVD (D)."

that is

$$C \longleftrightarrow D$$

Math vs. English

Mathematician: "If a function is not continuous (C), then it is not differentiable (D)."

$$\neg C \longrightarrow \neg D$$

Math vs. English

Mathematician: "If a function is not continuous (C), then it is not differentiable (D)."

$$C \longrightarrow D \;?\; \text{NO!}$$

Deductions

From: P implies Q, Q implies R

Conclude: P implies R

$$\frac{\overbrace{(P \to Q),\ (Q \to R)}^{\textit{Antecedents}}}{\underbrace{P \to R}_{\textit{Conclusion}}}$$

Sound Rules

Definition: A rule is *sound* if the conclusion is true whenever all antecedents are true.

A Sound Deduction

$$\frac{P \to Q, \quad P}{Q}$$

Modus ponens

A Sound Deduction

$$\frac{1 = -1}{\text{Russell is the Pope}}$$

An Unsound Deduction

$$\frac{\overline{P} \to \overline{Q}}{P \to Q}$$

An Unsound Deduction

not Smart → not MIT-student — Yes!

Smart → MIT-student — No!

Team Problem

Problems 2 & 3

